

Additive Bases of Vector Spaces over Prime Fields

N. ALON*

*Department of Mathematics, Sackler Faculty of Exact Sciences,
Tel Aviv University, Tel Aviv, Israel and
Bellcore, Morristown, New Jersey 07960*

N. LINIAL

*Department of Computer Science, Hebrew University of Jerusalem,
Jerusalem, Israel and
IBM Almaden Research Center,
650 Harry Road, San Jose, California 95120*

AND

R. MESHULAM†

*RUTCOR, Rutgers University, New Brunswick,
New Jersey 08903 and Department of Mathematics,
M.I.T., Cambridge, Massachusetts 02139*

Communicated by the Managing Editors

Received November 1, 1988

It is shown that for any $t > c_p \log n$ linear bases B_1, \dots, B_t of Z_p^n their union (with repetitions) $\bigcup_{i=1}^t B_i$ forms an additive basis of Z_p^n ; i.e., for any $x \in Z_p^n$ there exist $A_1 \subset B_1, \dots, A_t \subset B_t$ such that $x = \sum_{i=1}^t \sum_{y \in A_i} y$. © 1991 Academic Press, Inc.

1. INTRODUCTION

Let Z_p^n be the n -dimensional linear space over the prime field Z_p . An additive basis of Z_p^n is a multiset $\{x_1, \dots, x_m\} \subset Z_p^n$, such that any $x \in Z_p^n$ is representable as a 0-1 combination of the x_i 's. Let $f(p, n)$ denote the minimal integer t , such that for any t (linear) bases B_1, \dots, B_t of Z_p^n , the union (with repetitions) $\bigcup_{i=1}^t B_i$ forms an additive basis of Z_p^n .

The problem of determining or estimating $f(p, n)$, besides being interesting in its own right, is naturally motivated by the study of universal

* Research supported in part by Alon Fellowship and by a Bat Sheva de Rothschild Grant.

† Research supported in part by Air Force Office of Scientific Research Grant AFOSR-0271.

flows in graphs (see [JLPT]). The authors of [JLPT] conjectured that $f(p, n)$ is bounded above by a function of p alone.

Clearly $f(p, n) \geq p - 1$, as the union of $p - 2$ identical copies of the same basis does not form an additive basis. For $p \geq 3$ and $n \geq 2$, this trivial lower bound may be improved to $f(p, n) \geq p$. It clearly suffices to show this for $n = 2$. Let $\{a_1, a_2\}$ be any basis of Z_p^2 , and consider $p - 2$ copies of $\{a_1, a_2\}$ and one copy of $\{a_1 + a_2, a_1 - a_2\}$. As $-a_2$ is not in the additive span of these $p - 1$ bases we obtain $f(p, 2) \geq p$.

In this paper we give two proofs of the following.

THEOREM 1.1. $f(p, n) \leq c(p) \log n$.

In Section 2 we use exponential sums to show that $f(p, n) \leq 1 + (p^2/2) \log 2pn$. The algebraic method in Section 3 gives the somewhat better bound $f(p, n) \leq (p - 1) \log n + p - 2$. The final Section 4 contains some concluding remarks and open problems.

2. ADDITIVE SPANNING AND EXPONENTIAL SUMS

Let B_1, \dots, B_t be any $t > (p^2/2) \log 2pn$ bases of Z_p^n . Denote by $\{x_1, \dots, x_m\}$, $m = tn$, their union with repetitions, and for any $x \in Z_p^n$, let $N(x) = |\{(\varepsilon_1, \dots, \varepsilon_m) : \sum_{j=1}^m \varepsilon_j x_j = x, \varepsilon_j \in \{0, 1\}\}|$.

We shall show that $N(x) > 0$ for all $x \in Z_p^n$. For $x, y \in Z_p^n$, $x \cdot y$ is their standard inner product, and for $a \in Z_p$ let $e(a) = e^{2\pi ia/p}$.

Following Baker and Schmidt [BS, p. 471] we represent $N(x)$ as an exponential sum,

$$\begin{aligned} N(x) &= \sum_{\varepsilon \in \{0, 1\}^m} \frac{1}{p^n} \sum_{y \in Z_p^n} e\left(y \cdot \left(\sum_{j=1}^m \varepsilon_j x_j - x\right)\right) \\ &= \frac{1}{p^n} \sum_{y \in Z_p^n} \overline{e(y \cdot x)} \sum_{\varepsilon \in \{0, 1\}^m} e\left(y \cdot \sum_{j=1}^m \varepsilon_j x_j\right) \\ &= \frac{1}{p^n} \sum_{y \in Z_p^n} \overline{e(y \cdot x)} \sum_{\varepsilon_1=0}^1 \cdots \sum_{\varepsilon_m=0}^1 \prod_{j=1}^m e(\varepsilon_j y \cdot x_j) \\ &= \frac{2^m}{p^n} \sum_{y \in Z_p^n} \overline{e(y \cdot x)} \prod_{j=1}^m \frac{1 + e(y \cdot x_j)}{2}. \end{aligned}$$

Therefore

$$\left|N(x) - \frac{2^m}{p^n}\right| \leq \frac{2^m}{p^n} \sum_{0 \neq y \in Z_p^n} \prod_{j=1}^m \left|\frac{1 + e(y \cdot x_j)}{2}\right|. \tag{2.1}$$

(The same estimate is also used in [BS].) Next we estimate the right hand side of (2.1). For any fixed basis B of Z_p^n , and $y \in Z_p^n$ let $P_B(y) = \prod_{b \in B} |(1 + e(y \cdot b))/2|$.

Since $P_B(y)$ depends only on the list of inner products $(y \cdot b : b \in B)$, it follows that the multiset $\{P_B(y) : y \in Z_p^n\}$ is independent of the choice of the basis B . Choosing $B = \{b_1, \dots, b_n\}$ to be the standard basis of Z_p^n , and noting that for $y = (y_1, \dots, y_n)$

$$\left| \frac{1 + e(b_j \cdot y)}{2} \right| = \left| \frac{1 + e(y_j)}{2} \right| = \left| \cos \frac{\pi y_j}{p} \right|,$$

we obtain

$$\begin{aligned} \sum_{y \in Z_p^n} \left| \prod_{j=1}^m \frac{1 + e(y \cdot x_j)}{2} \right| &= \sum_{y \in Z_p^n} \prod_{i=1}^l P_{B_i}(y) \\ &\leq \sum_{y \in Z_p^n} P_B(y)^l = \sum_{y \in Z_p^n} \prod_{j=1}^n \left| \cos \frac{\pi y_j}{p} \right|^l \\ &= \left(\sum_{k=0}^{p-1} \left| \cos \frac{\pi k}{p} \right|^l \right)^n \leq \left(1 + (p-1) \cos^l \frac{\pi}{p} \right)^n \\ &\leq \left(1 + p \left(1 - \frac{\pi^2}{4p^2} \right)^{(p^2/2) \log 2pn} \right)^n \\ &< \left(1 + \frac{1}{2n} \right)^n < e^{1/2}. \end{aligned} \tag{2.2}$$

Combining (2.1) and (2.2) we obtain

$$\left| N(x) - \frac{2^m}{p^n} \right| \leq \frac{2^m}{p^n} (e^{1/2} - 1) < \frac{2^m}{p^n}.$$

Hence $N(x) > 0$ for all $x \in Z_p^n$. ■

3. PERMANENTS AND VECTOR SUMS

In this section we present a second proof of Theorem 1.1, with a somewhat better estimate for $c(p)$. Specifically, we prove the following proposition.

PROPOSITION 3.1. *Let $A_1 = \{a^{11}, \dots, a^{1n}\}$, $A_2 = \{a^{21}, \dots, a^{2n}\}, \dots$, $A_l = \{a^{l1}, \dots, a^{ln}\}$ be l bases of the vector space Z_p^n . If*

$$\left(1 - \frac{1}{p-1} \right)^{l-p+2} n < 1 \tag{3.1}$$

then for any vector $b \in Z_p^n$ there are $\varepsilon_{ij} \in \{0, 1\}$ ($1 \leq i \leq l$, $1 \leq j \leq n$), such that $\sum_{i,j} \varepsilon_{ij} a^{ij} = b$. In particular, the conclusion holds provided $l \geq (p-1) \log n + p - 2$.

The proof presented here differs considerably from the one given in Section 2 and is based on some simple properties of permanents over finite fields. The basic method resembles the one used in [AT], but several additional ideas are incorporated.

It is convenient to split the proof into several lemmas. We start with the following simple lemma (which appears in a similar context in [AFK]).

LEMMA 3.2. *Let $P = P(x_1, \dots, x_m)$ be a multilinear polynomial with m variables x_1, \dots, x_m over a commutative ring with identity R ; i.e., $P = \sum_{U \subseteq \{1, \dots, m\}} a_U \cdot \prod_{i \in U} x_i$, where $a_U \in R$. If $P(x_1, \dots, x_m) = 0$ for each $(x_1, \dots, x_m) \in \{0, 1\}^m$ then $P \equiv 0$, i.e., $a_U = 0$ for all $U \subseteq \{1, \dots, m\}$.*

Proof. We apply induction on m . The result is trivial for $m = 1$. Assuming it holds for $m - 1$ we prove it for m . Clearly $P(x_1, \dots, x_m) = P_1(x_1, \dots, x_{m-1})x_m + P_2(x_1, \dots, x_{m-1})$, where P_1 and P_2 are multilinear polynomials in x_1, \dots, x_{m-1} . Moreover, it is easy to see that P_1 and P_2 satisfy the hypotheses of the lemma for $m - 1$. By the induction hypothesis $P_1 \equiv P_2 \equiv 0$, completing the proof. ■

The next lemma shows a connection between a permanent of a matrix and the possible sums of subsets of its set of columns. This connection is crucial for our proof.

LEMMA 3.3. *Let $A = (a_{ij})$ be an m by m matrix over the finite prime field Z_p . Suppose that $\text{Per}(A) \neq 0$ (over Z_p). Then for any vector $c = (c_1, \dots, c_m) \in Z_p^m$ there are $\varepsilon_1, \dots, \varepsilon_m \in \{0, 1\}$ such that $\sum_{j=1}^m \varepsilon_j a_{ij} \neq c_i$ for all $1 \leq i \leq m$. In other words, for any vector c there is a subset of the columns of A whose sum differs from c in each coordinate.*

Proof. Suppose the lemma is false and let $A = (a_{ij})$ and c be a counter-example. Consider the polynomial $P = P(x_1, \dots, x_m) = \prod_{i=1}^m (\sum_{j=1}^m a_{ij}x_j - c_i)$. By assumption, $P(x_1, \dots, x_m) = 0$ for each $(x_1, \dots, x_m) \in \{0, 1\}^m$. Let $\bar{P} = \bar{P}(x_1, \dots, x_m)$ be the multilinear polynomial obtained from P by writing P as a sum of monomials and replacing each monomial $a_{ij} \prod_{i \in U} x_i^{\delta_i}$, where $U \subseteq \{1, \dots, m\}$ and $\delta_i > 0$, by $a_U \prod_{i \in U} x_i$. Clearly $\bar{P}(x_1, \dots, x_m) = P(x_1, \dots, x_m) = 0$ for each $(x_1, \dots, x_m) \in \{0, 1\}^m$. By Lemma 3.2 we conclude that $\bar{P} \equiv 0$. However, this is impossible, since the coefficient of $\prod_{i=1}^m x_i$ in \bar{P} (which equals the coefficient of that product in P) is $\text{Per } A \neq 0$. This completes the proof. ■

For a (column) vector $v = (v_1, \dots, v_n) \in Z_p^n$ let us denote by $v^* = v^*(p)$ the (column) vector in $Z_p^{(p-1)n}$ defined by $v_{(i-1)n+j}^* = v_j$ for all $1 \leq i \leq p - 1$,

$1 \leq j \leq n$. Thus v^* is simply the tensor product of v with a vector of $(p-1)1$'s. Clearly $v^* = v^*(p)$ depends on v as well as on p , but since p remains fixed during this section we usually omit it and simply write v^* .

A simple corollary of Lemma 3.3 is the following.

COROLLARY 3.4. *Let $\underline{a}^1, \dots, \underline{a}^{(p-1)n}$ be $(p-1)n$ vectors in Z_p^n . Let A be the $(p-1)n$ by $(p-1)n$ matrix whose columns are the vectors $\underline{a}^{1*}, \dots, \underline{a}^{(p-1)n*}$. If $\text{Per } A \neq 0$ then any vector $\underline{b} \in Z_p^n$ is a sum of a certain subset of the vectors $\underline{a}^1, \dots, \underline{a}^{(p-1)n}$.*

Proof. Let $\underline{c} = (c_1, \dots, c_{(p-1)n}) \in Z_p^{(p-1)n}$ be a vector satisfying $\{c_{(i-1)n+j} : 1 \leq i \leq p-1\} = Z_p \setminus \{b_j\}$ for each $j, 1 \leq j \leq n$. By Lemma 3.3 there are $\varepsilon_1, \dots, \varepsilon_{(p-1)n} \in \{0, 1\}$ such that for any $1 \leq i \leq p-1$ and any $1 \leq j \leq n$

$$\sum_{l=1}^{(p-1)n} \varepsilon_l \underline{a}_{(i-1)n+j}^{l*} \neq c_{(i-1)n+j}.$$

However, since the left hand side in the last equality is simply $\sum_{l=1}^{(p-1)n} \varepsilon_l \underline{a}_j^{l*}$ this shows that $\sum_{l=1}^{(p-1)n} \varepsilon_l \underline{a}_j^{l*} \notin Z_p \setminus \{b_j\}$ for each $1 \leq j \leq n$. Consequently, $\sum_{l=1}^{(p-1)n} \varepsilon_l \underline{a}^l = \underline{b}$, completing the proof. ■

The last corollary implies that in order to prove Proposition 3.1 it suffices to show that from any sequence of $l \cdot n$ vectors consisting l bases of Z_p^n one can choose $(p-1)n$ distinct members $\underline{a}^1, \dots, \underline{a}^{(p-1)n}$ of the sequence such that the permanent of the matrix whose columns are $\underline{a}^{1*}, \dots, \underline{a}^{(p-1)n*}$ is nonzero (over Z_p). In what follows we show that this is always possible provided (3.1) holds.

LEMMA 3.5. *Let $D = \{\underline{d}^1, \dots, \underline{d}^n\}$ be a basis of Z_p^n , and let A_D be a $(p-1)n$ by $(p-1)n$ matrix whose columns are the vectors $\underline{d}^{1*}, \dots, \underline{d}^{n*}$, each appearing $p-1$ times. Then $\text{Per } A_D \neq 0$.*

Proof. Let $E = \{\underline{e}^1, \dots, \underline{e}^n\}$ be the standard basis of Z_p^n , and let A_E be the $(p-1)n$ by $(p-1)n$ matrix whose columns are $\underline{e}^{1*}, \dots, \underline{e}^{n*}$, each appearing $(p-1)$ times. One can easily check that $\text{Per } A_E$ is simply the number of perfect matchings in the union of n pairwise disjoint complete bipartite graphs $K_{p-1, p-1}$, which is $((p-1)!)^n \neq 0$ (in Z_p). Since D is a basis, each column of A_E is a linear combination of the columns of A_D . By the multilinearity of the permanent function it follows that $\text{Per } A_E$ is a linear combination (over Z_p) of permanents of matrices whose columns are columns of A_D . Since $\text{Per } A_E \neq 0$, we conclude that there is a $(p-1)n$ by $(p-1)n$ matrix M , each column of which is \underline{d}^{i*} for some $1 \leq i \leq n$, satisfying $\text{Per } M \neq 0$. However, if the same column appears in M p times or more,

than $\text{Per } M$ is divisible by $p!$, and is thus 0. It follows that no column appears in M more than $(p-1)$ times, and hence M equals A_D up to a permutation of the columns. Thus $\text{Per } A_D = \text{Per } M \neq 0$, completing the proof. ■

LEMMA 3.6. Let $A_1 = \{a^{11}, a^{12}, \dots, a^{1n}\}, \dots, A_l = \{a^{l1}, a^{l2}, \dots, a^{ln}\}$ be l bases of Z_p^n and let $S = (\underline{s}_1, \dots, \underline{s}_n)$ be the sequence of length $l \cdot n$ of vectors in $Z_p^{(p-1)n}$ given by $\underline{s}_{(i-1)n+j} = a^{ij*}$ for all $1 \leq i \leq l, 1 \leq j \leq n$. Suppose that for some integer h

$$\left(1 - \frac{1}{p-1}\right)^{l-h} \cdot (p-1) \cdot n < h+1. \tag{3.2}$$

Then there are $(p-1)n$ distinct indices $1 \leq i_1 < i_2 < \dots < i_{(p-1)n} \leq ln$ such that the matrix whose columns are $\{\underline{s}_{ij} : 1 \leq j \leq (p-1)n\}$ has a nonzero permanent.

Proof. Given a $(p-1)n$ by $(p-1)n$ matrix B whose columns are members of S , we call a column of B a *repeated column* if the same member of S appears in at least one additional column of B . Let $c(B)$ denote the total number of repeated columns of B . Our objective is to construct a matrix with no repeated columns whose permanent is nonzero. To this end, we construct a sequence of matrices B_1, B_2, \dots , with nonzero permanents as follows. Let B_1 be the $(p-1)n$ by $(p-1)n$ matrix whose columns are $\underline{s}_1, \dots, \underline{s}_n$, each appearing $(p-1)$ times. By Lemma 3.5 $\text{Per } B_1 \neq 0$, and clearly, all the $(p-1)n$ columns of B_1 are repeated columns. Since A_2 is a basis, each column of B_1 is a linear combination of $\underline{s}_{n+1}, \dots, \underline{s}_{2n}$. Let us replace all but one of the $p-1$ occurrences of each \underline{s}_i in B_1 by the linear combination of $\underline{s}_{n+1}, \dots, \underline{s}_{2n}$ expressing it. By the multilinearity of the permanent function, this enables us to write $\text{Per } B_1 \neq 0$ as a linear combination of permanents of matrices whose columns are all from the set $\{\underline{s}_1, \dots, \underline{s}_{2n}\}$. Obviously, at least one of these matrices has a nonzero permanent. Let B_2 be such a matrix. Then, there are at least n nonrepeated columns of B_2 , since each of the n vectors $\underline{s}_1, \dots, \underline{s}_n$ appears precisely once in it. Hence, $c(B_2) \leq (1 - 1/(p-1))(p-1)n$. It is also clear that no \underline{s}_i appears more than $p-1$ times as a column of B_2 , as $\text{Per}(B_2) \neq 0$. Assume, by induction, that we have already constructed, for each $i \leq k$, a $(p-1)n$ by $(p-1)n$ matrix B_{i+1} , each column of which belongs to the set $\underline{s}_1, \dots, \underline{s}_{(i+1)n}$, satisfying

$$\text{Per}(B_{i+1}) \neq 0 \quad \text{and} \quad c(B_{i+1}) \leq \left(1 - \frac{1}{p-1}\right)^i (p-1)n. \tag{3.3}$$

Let us show that if $k+2 \leq l$ we can construct a matrix B_{k+2} with the same properties. If $c(B_{k+1}) = 0$ simply take $B_{k+2} = B_{k+1}$. Otherwise, replace

each occurrence of each repeated column of B_{k+1} but one, by a linear combination of $\underline{s}_{(k+1)n+1}, \dots, \underline{s}_{(k+2)n}$ and apply, as before, multilinearity to obtain a matrix B_{k+2} with a nonzero permanent. Since no repeated column can appear in B_{k+1} more than $p-1$ times, we conclude that

$$c(B_{k+2}) \leq \left(1 - \frac{1}{p-1}\right) c(B_{k+1}) \leq \left(1 - \frac{1}{p}\right)^{k+1} (p-1)n.$$

In particular, taking $i = l-h$, it follows from (3.2) and (3.3) that there is a matrix B_{l-h+1} , each column of which belongs to the set $\underline{s}_1, \dots, \underline{s}_{(l-h+1)n}$ such that $\text{per}(B_{l-h+1}) \neq 0$ and $c(B_{l-h+1}) \leq (1 - 1/(p-1))^{l-h} (p-1)n < h+1$.

Thus B_{l-h+1} has at most h repeated columns. Denote these columns by $\underline{b}^l, \underline{b}^{l-1}, \dots, \underline{b}^{l-h+1}$. For each $i, 0 \leq i \leq h-2$, let us express \underline{b}^{l-i} as a linear combination of $\underline{s}_{(l-i-1)n+1}, \dots, \underline{s}_{(l-i)n}$. Applying multilinearity once more we obtain a matrix with nonzero permanent and no repeated columns. This completes the proof. ■

We are now ready to prove Proposition 3.1. Given the l bases A_1, \dots, A_l , where l satisfies (3.1), we apply Lemma 3.6 with $h = p-2$ to conclude that there is a set I of $(p-1)n$ distinct double indices ij such that the matrix whose columns are $\{a^{ij*} : ij \in I\}$ has a nonzero permanent. By Corollary 3.4, this implies that for any vector $\underline{b} \in Z_p^n$ there are $\varepsilon_{ij} \in \{0, 1\}, (ij \in I)$, such that $\sum_{ij \in I} \varepsilon_{ij} a^{ij} = \underline{b}$. This completes the proof of Proposition 3.1. Observe that we actually proved a somewhat stronger result; if l satisfies (3.1) then it is possible to choose a fixed set of $(p-1)n$ of our vectors such that any $\underline{b} \in Z_p^n$ is a sum of a subset of this fixed set. ■

4. CONCLUDING REMARKS AND OPEN PROBLEMS

The main open problem is, of course, whether the union of any $c(p)$ linear bases of Z_p^n is an additive basis, where $c(p)$ depends on p alone. The following two results, which follow from our previous proofs of Theorem 1.1, suggest that this, indeed, may be the case.

PROPOSITION 4.1. *For any l bases B_1, \dots, B_l of Z_p^n , when $l \geq p \log(pn)$ there are subsets $A_i \subset B_i$ ($1 \leq i \leq l$), such that $\sum_{i=1}^l |A_i| \leq (p-1)n$ and $\bigcup_{i=1}^l A_i$ (with repetitions) is an additive basis of Z_p^n .*

PROPOSITION 4.2. *Let $S = (s_1, s_2, \dots, s_l)$ be a sequence of vectors in Z_p^n and suppose that each subsequence of $l - (p-1)n$ members of S linearly spans Z_p^n . Then S is an additive basis of Z_p^n .*

The following conjecture about permanents would imply, if true, that $f(p, n) \leq p$.

CONJECTURE 4.3. For any p nonsingular n by n matrices A_1, A_2, \dots, A_p over Z_p , there is an n by $p \cdot n$ matrix C such that

$$\text{Per} \begin{bmatrix} A_1 A_2 \cdots A_p \\ A_1 A_2 \cdots A_p \\ \vdots \\ A_1 A_2 \cdots A_p \\ C \end{bmatrix} \neq 0.$$

REFERENCES

- [AFK] N. ALON, S. FRIEDLAND, AND G. KALAI, Regular subgraphs of almost regular graphs, *J. Combin. Theory Ser. B* **37** (1984), 79–91.
- [AT] N. ALON AND M. TARSI, A nowhere zero point in linear mappings, *Combinatorica* **9** (1989), 393–395.
- [BS] R. C. BAKER AND W. M. SCHMIDT, Diophantine problems in variables restricted to the values 0 and 1, *J. Number Theory* **12** (1980), 460–486.
- [JLPT] F. JAEGER, N. LINIAL, C. PAYAN AND M. TARZI, Group connectivity of graphs—a nonhomogeneous analogue of nowhere-zero flow, *J. Combin. Theory Ser. B*, to appear.